Security Statement

Landmark National Bank's online banking and bill pay system brings together a combination of industry-approved security technologies to protect data for the bank and for you, our customer. To begin a session with the bank's server the user must key in a Log-in ID and a password. Our online banking and bill pay system uses a "3 strikes and you're out" lock-out mechanism to deter unauthorized users from repeated login attempts. After three unsuccessful login attempts, the system locks the user out. Upon successful login, the system authenticates the user's identity and establishes a secure session with that user. Once the server session is established, the user and the server are in a secured environment, and data traveling between the user and the server is encrypted.

Regulation E

Landmark National Bank is required under Regulation E: Electronic Fund Transfers to provide certain protections to our retail customers relative to electronic fund transfers (EFT). As applicable to online access, this regulation covers transactions initiated through Landmark National Bank's online banking, to either order, instruct, or authorize the financial institution to debit or credit an account. Transactions may include but are not limited to ACH payments, external transfers, and bill payments. For specific applicability and provisions, please request a copy of Landmark National Bank's EFT disclosure by calling 800-318-8997.

Request for information

Landmark National Bank will NEVER request a customer's personal information (debit card number, account number, social security number, personal identification number or password) through email or by phone. If you ever receive an unsolicited phone call or email claiming to be from Landmark National Bank requesting your personal and confidential information, please DO NOT respond. Contact us immediately by calling 800-318-8997. As an additional monitoring control, you should review account statements and online account transaction history to ensure all transactions are correct and authorized.

E-mail and electronic communications

E-mail transmitted across the Internet is normally not encrypted and may be intercepted by third parties. Customers should therefore avoid sending any confidential or private information in e-mails to Landmark National Bank. Likewise, Landmark National Bank will not include confidential information in any e-mailed response to you.

Timeout feature

Landmark National Bank's online banking has a timeout feature which automatically logs out the user from the current online banking session after an extended period of inactivity. Because someone else might obtain physical access to a customer's system, it is better for privacy reasons to exit the online banking session after all activity is finished, rather than waiting for the timeout feature to occur.

Passwords

As stated previously, the online banking system requires the use of a password to gain access. The password must be between 8 and 16 characters in length. Passwords must contain letters, numbers, and at least one capital letter. Your password should not be associated with any commonly known personal identification, such as social security numbers, address, date of birth or names of children, and should be memorized rather than written down.

Risk Assessments

Landmark National Bank is required by its banking regulators to conduct regular periodic risk assessments of their electronic banking products and services to identify security threats, and implement controls to mitigate the risks associated with those threats. As a proactive measure, we strongly suggest to our business or commercial customers to also perform a periodic risk assessment and controls evaluation related to security of their internet banking / cash management environment. Special attention should be directed to high risk transactions which involve access to personal financial information or the movement of funds to other parties such as ACH, wire transfers, and bill payment.

System Access Restrictions

Landmark National Bank can terminate or limit your access to the online banking and bill pay system at any time with or without cause. Or at any time it is deemed necessary to maintain the security of an Account or our online banking and bill pay system.

Activity Reports

Landmark National Bank has implemented strong preventative and monitoring controls within its online banking and bill pay system. We review activity reports to find anything that appears out of the ordinary. We look at specific information to investigate activities that appear suspicious and to protect our systems and personal information. However, in order to enhance our customer's internal security we recommend our customers implement their own controls to mitigate risks. Examples of controls you may want to consider implementing to mitigate the risks of fraudulent account activities are as follows:

- Maintain up-to-date operating system security patches and install virus/spyware protections software. Viruses and spyware can leave your computer vulnerable to attack and intrusion. Anti-virus and anti-spyware software will help to keep your computer safe from malicious software that could install itself or may try to install itself on your computer.
- Install a Firewall, either software or hardware. A firewall will prevent attacks on your computer through the Internet using established rules to determine if a requested connection is malicious or not.
- Implement intrusion detection/prevention software or services.
- Safekeeping and confidentiality of Internet banking authentication credentials.
- For business customers, implement dual control for initiating and approving high risk Cash Management transactions such as ACH origination and wire transfers.
- Daily account activity monitoring via Internet banking account transaction history review.
- Review and monitor your checking account, debit card, and credit card statements for unauthorized transactions.
- Refrain from opening unsolicited email and attachments.
- Refrain from providing authentication credentials to callers claiming to be representing the financial institution and from responding to emails requesting information or re-directing you to a website.
- Prior to disposing, shred all confidential information on hardcopy and on electronic media.

If you notice any suspicious or unauthorized account activity, experience a breach in security of personal information, your login credentials or computer security have been compromised, or for more information please contact Landmark National Bank immediately at 800-318-8997.